

Maker 多担保 Dai (MCD) 系统白皮书

原文链接: makerdao.com

翻译: 闵敏、阿剑

校对: 潘超

两位译者系 EthFans.org (以太坊爱好者) 成员; 校对系 MakerDAO 中国区负责人

摘要

Maker 协议, 又称多担保 Dai (MCD) 系统, 可以让用户使用经过 “Maker 治理 (Maker Governance)” 批准的资产作为担保物来生成 Dai。Maker 治理是由社区组织并运营的一套管理 Maker 协议各方面的流程。Dai 是一种软锚定美元的资产担保型加密货币, 其发行是去中心化、一视同仁的。由于波动性低, Dai 能够抵御恶性通货膨胀, 并为全球范围内的任意个体提供经济自由和机会。

本白皮书从通俗易懂的角度讲解了构建在以太坊区块链上的 Maker 协议。精于技术的读者可以直接阅读 Maker 文档页面 (Maker Documentation Portal) 中的 [《Maker 协议介绍》](#), 深入理解整个系统。

关于 MakerDAO

MakerDAO 是 2014 年在以太坊区块链上创建的开源去中心化自治组织¹。该项目发行一种名为 MKR 的治理型代币, 全世界范围内持有该代币的人均可参与项目治理。通过由执行投票 (Executive Voting) 和治理投票 (Governance Polling) 组成的[科学型治理系统](#), MKR 持有者可以管理 Maker 协议及 Dai 的金融风险, 从而确保该协议的稳定性、透明性和高效性。MKR 投票权重与投票者存在投票合约 DSChief 中的 MKR 数量成正比。换言之, 投票者在 DSChief 合约中锁定的 MKR 代币数量越多, 其拥有的决策权就越大。

关于 Maker 协议

Maker 协议构建在以太坊区块链²上, 用户可以用其创造货币。该协议目前由稳定币 Dai、Maker Collateral Vault (Maker 担保物金库)、信息输入系统 (Oracle, 旧译作 “预言机”) 和投票机制组成。MakerDAO 依靠 MKR 持有者的投票决定关键的参数 (例如, 稳定费率、担保物类型/质押比率等), 来治理 Maker 协议。

Maker 协议是以太坊区块链上最大的去中心化应用 (dApp) 之一, 也是第一个获得大规模采用的去中心化金融 (DeFi) 应用。

关于 Maker 基金会

[Maker 基金会](#) 是全球 Maker 社区的一部分, 与许多外部合作伙伴一起创建了 Maker 协议。Maker 基金会与 MakerDAO 社区合作, 引导 MakerDAO 项目的去中心化治理, 并推动其实现完全的去中心化。关于 Dai 基金会Dai 基金会是位于丹麦的自治组织, 独立于 Maker 基金会。Dai 基金会负责管理 Maker 社区的重要无形资产, 例如, 商标和代码版权, 依据定义了其权限的严格规章来运行。正如 [Dai 基金会委托书](#) 中所言, 该基金会的目的是保护 Maker 协议中无法通过技术实现去中心化的部分。

引言

从 2015 年开始, MakerDAO 与来自全球的开发者开始了对代码、架构和文档的第一版迭代。在 2017 年 12 月, [MakerDAO 发布了第一版正式白皮书](#), 介绍了最初的 Dai (也就是如今的 Sai) 稳定币系统。

该白皮书介绍了通过名为担保债仓（Collateralized Debt Position, CDP）的独特智能合约 来质押以太币（ETH）生成 Dai 的系统。鉴于以太币是该系统唯一接受的担保资产，生成的 Dai 被称为单担保 Dai（Single-Collateral Dai, SCD），现又称 Sai。该白皮书还提到了升级该系统的计划，支持包括以太币在内的多种担保资产。该计划已于 2019 年 11 月落实。

Dai 稳定币系统，现称 Maker 协议，目前接受所有基于以太坊、且经过 MKR 持有者批准的资产作为担保物，MKR 持有者还有权投票决定每种担保物的风险参数（Risk Parameter）。投票机制是 Maker 去中心化治理流程的关键一环。

欢迎使用多担保 Dai（MCD）

区块链技术提供了前所未有的机会，来解决公众对功能失调的中心化金融系统的不满和不信任。通过将数据分布到计算机网络中，该技术可以让任意团体中的每位成员都享有透明性，不受中心实体的控制，由此诞生出无偏袒、透明且高效的免许可型系统——可以改善当前的全球金融和货币结构，更好地为公众利益服务。

比特币就是为此而创建的。虽然比特币从许多方面来说都是一种成功的密码学货币，但是它并不是一种理想的交换媒介，因为它的供应量是固定的，它的投机性又造成了价格的波动，使其无法进一步发展成为主流货币。

另一方面，比特币的短板恰好是 Dai 稳定币优势，正是因为它的设计目标就是将价格波动性降至最低。Dai 是一种去中心化且中立的资产担保型加密货币，其价格软锚定美元。稳定性是 Dai 的意义。

自单担保 Dai 于 2017 年上线之后，[用户接受度不断提高](#)，已成为去中心化金融 dApp 的基石。Dai 的成功也是整个稳定币行业运动的一部分，稳定币是旨在维持价格和货币功能的加密货币。

例如，在 2019 年 2 月，摩根大通（JPMorgan）成为了美国第一家创建并测试锚定美元的数字货币的银行³。随着数字货币行业的发展，一些银行、金融服务公司，甚至是政府都想创建稳定型数字货币（例如，中央银行数字货币），非金融领域的大型公司也是如此。例如，Facebook 就在 2019 年 6 月宣布了 Libra（由等额实物资产背书的稳定型数字货币）计划⁴。但是，这类提议违背了区块链技术的核心价值主张：建立一个不受中心化权力机构或管理者影响的公共基础设施，并在全球范围内采用。

Maker 协议及其特征概述

Maker 协议

Maker 协议是以太坊区块链上最大的去中心化应用之一。参与设计该协议的人员非常多样化，包括 Maker 基金会的开发者、外部合作伙伴，以及其他个人和实体。Maker 协议是首个获得大规模采用的去中心化金融（DeFi）应用。

Maker 协议由世界各地的治理型代币 MKR 持有者管理。通过由执行投票（Executive Voting）和治理投票（Governance Polling）组成的[科学型治理系统](#)，MKR 持有者可以管理 Maker 协议及 Dai 的金融风险，从而确保该协议的稳定性、透明性和高效性。投票合约中锁定的每一个 MKR 代币均等同于一票。

稳定币 Dai

稳定币 Dai 是一种软锚定美元的资产担保型加密货币，其发行是去中心化、无偏见的。Dai 已在以太坊区块链和一些其他流行的区块链上发行；持有 Dai 需要用到加密货币钱包 或者 加密资产平台。

Dai 的生成、访问和使用门槛都很低。用户通过使用 Maker 协议来创建叫做“Maker Vault（Maker 金库）”的智能合约并存入资产来生成 Dai。这个过程既是 Dai 进入流通领域的过程，也是用户获得流动性的过程。此外，用户也可以从中介或交易所处购买 Dai；或者更简单一点，只要愿意接受 Dai 来支付，那就能得到 Dai。

无论是你自己生成的、买到的还是收到的 Dai，用起来都跟别的加密货币没有区别：你可以将 Dai 发送给其他人，用它来购买商品和服务，甚至可以通过叫做“Dai 存款利率 (Dai Savings Rate, DSR)”的 Maker 协议功能，把 Dai 转入储蓄账户。

流通中的每个 Dai 都是由超额资产背书的——担保物的价值总是高于 Dai 债务的价值——而且所有 Dai 交易都在以太坊区块链上公开可见。

Dai 有哪些类似于货币的功能？

通常来说，货币有四大功能：

1. 价值贮藏
2. 交换媒介
3. 记账单位
4. 延期支付标准

为了满足上述功能，Dai 专门设计了以下特点和应用场景。

Dai 是一种价值贮藏物

价值贮藏物指的是能够保值的资产，不会随时间流逝而大幅贬值的资产。Dai 是一种稳定币，其设计使其在波动巨大的市场中也能保证价格稳定。

Dai 是一种交换媒介

交换媒介指的是一切可代表价值标准、被用来促进商品或服务的出售、购买或交换（交易）的事物。在全世界不同类型的交易中，都能使用 Dai 稳定币来达成交易。

Dai 是一种记账单位

记账单位是一种标准化的价值度量衡（例如，美元、欧元、日元），用于商品和服务的定价。目前，Dai 的目标价格是 1 USD（1 Dai = 1 USD）。虽然 Dai 尚未在区块链外成为标准的价值度量衡，但是它在 Maker 协议和一些区块链 dApp 中充当记账单位之用。其中，Maker 协议的记账和 dApp 服务的定价采用的都是 Dai 而非美元之类的法币。

Dai 是一种延期支付标准

在 Maker 协议中，Dai 还被用来清偿债务（例如，用户使用 Dai 来支付稳定费并关闭金库）。正是这一优势使得 Dai 如此出众。

担保品资产

Dai 的创造、价值背书、价格稳定，都是通过存入 Maker 金库的担保品资产来实现的。担保品资产指的是由 MKR 持有者投票纳入协议的数字资产。

只要经过 MKR 持有者的批准，任何基于以太坊的资产都可以在 Maker 协议上用作生成 Dai 的担保物。在许可某种资产成为担保品时，MKR 持有者还必须相应选择具体的风险参数（例如，稳定型资产可能要选择较为宽松的风险参数，风险型资产可能要选择较为严格的风险参数。）关于风险参数的具体内容请参见下文。MKR 持有者是通过 Maker 去中心化治理流程做出上述以及其他决策的。

Maker 金库

所有经过批准的担保品资产都可以存入使用 Maker 协议生成的 Maker 金库智能合约来生成 Dai。用户可以通过多种用户界面（即网络访问门户）访问 Maker 协议并创建金库。这些用户界面包括 [Oasis Borrow](#) 以及 [由社区构建的各种界面](#)。创建金库并不复杂，但是生成 Dai 意味着用户对系统有了一笔债务；需要归还 Dai 并支付稳定费，才能取回金库中锁定的担保物。

金库本质上是非托管型的：用户可与金库和 Maker 协议直接交互。只要担保物的价格不低于最低必要水平（即清算率（Liquidation Ratio），详见下文），用户即享有对该担保物完整且独立的控制权。

如何与 Maker 金库交互

- **步骤一：创建金库并锁入担保物**

用户通过 Oasis Borrow 门户或 Instadapp、Zerion、MyEtherWallet 等由社区创建的界面来创建 金库，并锁入特定类型和数量的担保物来生成 Dai。存入资金之时，该金库即被视为有担保的。

- **步骤二：通过有担保的金库生成 Dai**

将担保品资产锁入一个金库之后，该金库所有者便可使用任意非托管型密码货币钱包来发起、确认交易，生成出一定数量的 Dai。

- **步骤三：偿还债务并支付稳定费**

若想取回部分或所有担保物，金库所有者必须部分或全额偿还 TA 所生成的 Dai，并支付 Dai 未偿还期间不断累积的稳定费。稳定费只能用 Dai 支付。

- **步骤四：取出担保物**

在偿还了 Dai 并支付了稳定费之后，金库所有者可以将部分或全部担保物退回自己的钱包。在完全偿还了 Dai 并取出所有担保物之后，金库就会空置下来，以待其所有者再次锁入资产。

尤为关键的是，不同的担保品资产需分置在不同的金库中。因此，一些用户会拥有多个金库，采用的担保物类型和担保品率各不相同。

高风险 Maker 金库的清算

为了确保 Maker 协议中始终有充足的担保物来为未偿还债务背书（未偿还债务即以目标价格（Target Price）计算的未偿还 Dai 的总价值），任何（根据 Maker 治理规定的参数）被判定为高风险的 Maker 金库都会通过自动化的 Maker 协议拍卖流程来清算。Maker 协议的判定依据是比较清算率与该金库当前的担保品价值-债务比率（collateral-to-debt ratio）。每种金库类型都有各自的清算率，是 MKR 持有者基于不同担保品资产的风险状况投票决定的。

Maker 协议拍卖

通过 Maker 协议的[拍卖机制](#)，系统在无法获得担保物的价格信息之时依然能对金库进行清算。在进行清算之时，Maker 协议会取出被清算的金库中的担保物，并使用协议内一个基于市场的拍卖机制将其卖出。这被称为担保品拍卖（Collateral Auction）。

通过担保物拍卖获得的 Dai 会被用来偿还金库内的债务，其中包括清算罚金（Liquidation Penalty）。MKR 投票者会针对不同的担保物类型设定不同的清算罚金。

如果担保物拍卖上获得的 Dai 足以清偿金库内的债务，并足够支付清算罚金，该竞拍会转换成反向担保品竞拍（Reverse Collateral Auction）尽可能地减少担保物的出售数量。剩余的担保物都会物归原主。

如果担保物竞拍获得的 Dai 不足以清偿金库内的债务，亏损部分就会变成 Maker 协议的负债，由 Maker 缓冲金（Maker Buffer）中的 Dai 偿还。如果缓冲金中没有足够的 Dai，Maker 协议就会触发债务拍卖（Debt Auction）机制。在债务拍卖期间，系统会铸造新的 MKR（增加流通中的 MKR 量），出售给那些使用 Dai 来参与竞拍的用户。

担保物拍卖得到的 Dai 会进入 Maker 缓冲金。Maker 缓冲金可以起到缓冲的作用，避免将来因担保物竞拍不足和 Dai 存款利率上涨而导致 MKR 的增发量过大（详见下文）。

如果由竞拍和稳定费获得的 Dai 超过了 Maker 缓冲金的上限（由 Maker 治理设定的值），超出的部分就会通过盈余拍卖（Surplus Auction）出售。在盈余拍卖期间，投标者使用 MKR 来竞拍固定数量的 Dai，价高者得。一旦盈余拍卖结束，Maker 协议会自动销毁拍卖所得的 MKR，从而减少 MKR 的总供应量。

担保物拍卖流程示例：

由于市场行情的影响，某个大额金库的质押率跌至最低阈值以下。某个拍卖清算商（Auction Keeper）检测到这一现象并对该金库启动清算程序。假设有 50 ETH 进入拍卖流程。

每个清算商都可以有自己的[竞拍策略 \(bidding model\)](#)。竞拍策略中包含担保物（在本例中为 ETH）的竞标价。发起清算的清算商将自己竞拍策略中的代币价格作为担保物拍卖第一阶段的起拍价。在该阶段，投保者使用 Dai 来竞拍固定数量的担保物，价高者得。这个数量是不可分拆的，竞拍者出的价格就是总价。

设这个清算商要出 5000 Dai 去竞标 50 ETH。这部分 Dai 会从金库引擎转移到担保物竞拍合约内。等到某一笔充进担保物竞拍合约的 Dai 能够偿还系统的债务并支付清算罚金，担保物竞拍的第一阶段就结束了。

为了用自己竞拍策略中的价格买到担保品，清算商还要在担保物竞拍的第二阶段提交报价。这一阶段的目标是在市场竞争的情况下，将尽可能多的担保物归还给金库的所有者。在这一阶段，清算商要使用固定数量的 Dai 去竞拍尽可能少的 ETH。例如，在本例中，该清算商的竞拍策略所寻求的竞标价是 125 Dai/ETH，即，用 5000 Dai 去竞拍 40 ETH。本次竞标获得的 Dai 会从金库引擎转移到担保物竞拍合约内。等到投标期结束，竞标截止之后，该竞拍管理者中标，取得担保物。担保物竞拍彻底结束。

主要的外部参与者

除了智能合约基础设施之外，Maker 协议的运行还需要依靠各类外部参与者群体：看护者

（Keeper）、信息输入者（Oracle）、全局清算者（Global Settler，又称 Emergency Oracle，即，紧急信息输入者）和 Maker 社区成员。清算商是 Maker 协议经济激励机制的受益者；信息输入者和全局清算者都是享有特殊系统权限的外部参与者，其权限由 MKR 持有者通过投票赋予；Maker 社区成员是提供服务的个人和组织。

看护者（Keeper）

看护者是独立的（通常是自动化的）参与者，在套利机会的激励下为去中心化系统的各个方面提供流动性。在 Maker 协议中，[看护者指的是帮助 Dai 维持目标价格（1 美元）的市场参与者](#)：他们会在 Dai 的市场价格超出目标价格时将其卖出，并在市场价格低于目标价格之时买入。在 Maker 金库被清算之时参与盈余拍卖、债务拍卖和担保物拍卖的也称为看护者（清算商）。

价格信息输入机（Price Oracle）

Maker 协议需要实时了解 Maker 金库中充当担保物的资产的市场价格，从而知道何时触发清算机制。

Maker 协议的内部担保物价格来自[去中心化信息输入架构 \(decentralized Oracle infrastructure\)](#)。该架构由大量名为“喂价机（Oracle Feed）”的独立节点组成。MKR 投票者选出一组可信赖的喂价节点，并由通过以太坊交易向 Maker 系统提供价格信息。群组的节点数量也是由 MKR 投票者来控制的。

为了防范攻击者控制大部分喂价机的情况，Maker 协议是通过[喂价安全模块 \(Oracle Security Module, OSM\)](#)来获取价格信息的，并不直接通过喂价机获取。喂价安全模块是架设在喂价机节点和 Maker 协议之间的防御层，将价格更新延迟 1 小时。在此期间，如果有喂价机被攻击者控制，可通过紧急信息输入者或 Maker 治理投票将其冻结。紧急信息输入者以及价格输入时滞的决策权都在 MKR 持有者手里。

紧急信息输入者（Emergency Oracle）

紧急信息输入者是 MKR 持有者投票选出的，是保护治理流程和其他信息输入者免遭攻击的最后一道防线。紧急预言机能够冻结单个喂价机（例如，ETH 和 BAT 的喂价机），有权单方触发紧急关停机制（Emergency Shutdown）。以此降低大量客户试图在短时间内从 Maker 协议取回资产所产生的风险。

DAO 团队

DAO 团队是由个人和服务提供商组成的，通过 Maker 治理流程（Maker Governance）签订合同来向 MakerDAO 提供特定的服务。DAO 团队的成员都是独立的市场参与者，并非受雇于 Maker 基金会。

Maker 治理的灵活性使得 Maker 社区能够调整 DAO 团队框架，基于现实情况和新兴挑战来提供整个生态系统所需的服务。

DAO 团队的成员被划分为不同的角色。例如，治理协调员（Governance Facilitator），负责主持沟通和治理流程；风险团队（Risk Team）成员，通过金融风险研究和起草关于引入新型担保物和管理现有担保物的提案来支持 Maker 治理。

虽然 Maker 治理到目前为止都是由 Maker 基金会引导的，但是 DAO 有望在不久的将来充分掌握自主权，发起 MKR 投票来填充 DAO 团队中的各种角色。

Dai 存款利率（Dai Savings Rate, DSR）

[Dai 存款利率让所有 Dai 用户可以自动获得储蓄收益](#)，只需用户将他们的 Dai 锁入 Maker 协议的 DSR 合约即可，该合约可以通过 [Oasis 的存款平台](#)或[其他接入 Maker 协议的平台](#)访问。DSR 合约不对用户设置最低存款要求，用户可以随时从 DSR 合约中取出部分或全部 Dai。

DSR 是一个系统全局参数，决定了 Dai 持有者可基于其存款获得的收益。当 Dai 的市场价格由于市场变化而偏离目标价格时，MKR 持有者可以通过投票更改 DSR 来维护价格的稳定性：

- 如果 Dai 的市场价格超过 1 美元，MKR 持有者可以选择逐渐降低 DSR，以此减少需求量，进而将 Dai 的市场价格降至 1 美元的目标价格。
- 如果 Dai 的市场价格低于 1 美元，MKR 持有者可以选择逐渐增加 DSR，以此刺激需求量上升，进而将 Dai 的市场价格增至 1 美元的目标价格。

最初，每周都会有一个 DSR 调整流程。MKR 持有者首先评估并讨论市场参与者提供的公开市场数据和特定数据，然后再投票决定是否有必要调整 DSR。长期计划是实现 DSR 调整模块（DSR Adjustment Module），即一个可以直接控制 DSR 和基础利率（Base Rate）的即时访问模块（Instant Access Module）。通过该模块，单个 MKR 持有者可以代表一群 MKR 持有者轻松地调整 DSR（调整的幅度范围和频率范围由 MKR 持有者预先设定）。该计划旨在提高 DSR 对瞬息万变的状况的灵敏度，并避免过度使用执行投票和治理投票这两个标准治理流程。

Maker 协议的治理

MKR 代币在 Maker 治理中的使用

MKR 代币——Maker 协议的治理型代币——允许其持有者通过 *投票* 来修改 Maker 协议。要注意的是，不只是 MKR 持有者，任何人都可以 *提交* 提议来发起 MKR 投票。

对 Maker 协议治理型变量的更改在通过投票批准之后是不太可能立即生效的。如果投票者选择启动治理安全模块（Governance Security Module, GSM），这些更改就会被推迟激活（推迟最多 24 小时）。这段时间给了 MKR 持有者行动的机会，如有必要，他们可触发关停机制，来反对恶意的治理提议（例如，将担保物参数修改成与现行货币政策相悖的提议，或是关闭安全机制的提议）。

提议投票和执行投票

Maker 治理流程包括提议投票和执行投票。提议投票的目的是在进行执行投票之前，先在社区内形成一个大致的共识。这有助于确保治理决策是经过仔细考虑，且在进入投票流程之前就已达成一致的。执行投票的目的是 *批准/驳回* 对系统状态的更改，例如，投票决定新引入担保物的风险参数。

从技术层面来说，每一类投票都是由智能合约管理的。提议合约（Proposal Contract）是通过编程的方式写入了一个或多个有效治理行为的智能合约。提议合约只能执行一次。一旦执行了，它就会立即对 Maker 协议的内部治理变量进行更改。在执行之后，该提议合约就不能再度使用。

任意以太坊地址都可以部署有效的提议合约。MKR 代币持有者可以通过投批准票来选出有效提议（Active Proposal）。获得赞成票最多的以太坊地址的提议会被选为有效提议。有效提议会获得 Maker 协议的内部治理变量的管理权限，然后修改这些参数。

MKR 代币在资本重组中的作用

除了在 Maker 治理中的作用，MKR 代币还有一种辅助性作用是充当 Maker 协议的资本重组资源。如果系统债务超过了盈余，就会触发债务拍卖（参见上文）来增加 MKR 代币的供应量，对系统进行资本重组。这一风险会激励 MKR 持有者团结一致，负责地管理 Maker 的生态系统，避免过多风险的发生。

MKR 持有者的职责

MKR 持有者可以对以下事项进行票决：

- 引入新的担保物类型，并为其设置一组风险参数
- 修改、乃至增加一种或多种现有担保物资产类型的风险参数
- 修改 Dai 存款利率
- 选出喂价机节点群组
- 选出紧急信息输入者群组
- 触发紧急关停
- 升级系统

MKR 持有者可以用 Maker 缓冲金里的资金来支付各种基础设施方面的需求和服务，包括信息输入机制和担保物风险管理研究。Maker 缓冲金里的资金来自稳定费、清算费和其他收入来源。

Maker 协议治理机制的设计目标是尽可能灵活化，并具备可升级性。如果 Maker 系统在社区的引导下成熟起来，那么从理论上来说，提议合约的形式也会变得更高级，比如一个提议合约可以绑定多项提议。例如，提议合约可以同时包含对稳定费的调整 and DSR 的调整。不过，这些改进仍待 MKR 持有者共同决定。

由 Maker 治理控制的风险参数

每一种 Maker 金库（例如，ETH 金库和 BAT 金库）都有自己独特的风险参数集，而且是强制生效的。这些参数的决定依据是对担保品的风险预测，而且是直接由 MKR 持有者通过投票决定的。

以下是 Maker 金库的主要风险参数：

- **债务上限（Debt Ceiling）**：债务上限指的是一种担保品所能生成出债务总额上限。Maker 治理为每一种担保物都设定了债务上限，以确保 Maker 协议的担保物组合具备足够的多样性。一旦某种担保物达到了债务上限，就不可能产生更多债务，除非已有用户偿还部分或全部的金库债务（从而释放出债务空间）。
- **稳定费（Stability Fee）**：稳定费是根据一个金库所生成的 Dai 数量来计算的年利息（对生成 Dai 的用户来说，稳定费率相当于贷款的年化利率；对 Maker 协议来说，稳定费率相当于年化的收益率）。稳定费只能由 Dai 支付，发送至 Maker 缓冲金。
- **清算率（Liquidation Ratio）**：清算率较低，意味着 Maker 治理对担保物价格波动性的预期较低；清算率较高，意味着对价格波动性的预期较高。
- **清算罚金（Liquidation Penalty）**：清算罚金是当清算发生时，根据金库中未偿还 Dai 的总量向用户收取的额外一笔费用。清算罚金旨在鼓励金库所有者将质押率保持在适当的水平。
- **担保物拍卖期（Collateral Auction Duration）**：每种 Maker 金库的担保物拍卖时间上限都是特定的。债务拍卖期和盈余拍卖期则是系统全局参数。
- **竞拍期（Auction Bid Duration）**：单次竞拍结束及终结之前的最低时长。
- **最低加价幅度（Auction Step Size）**：这一风险参数旨在激励拍卖中的早期竞拍者，防止加价幅度过低的情况泛滥。

治理的风险和缓解措施

为了维护 Maker 协议的成功运行，Maker 治理需要采取必要的风险缓解措施。下文详细说明了一些风险以及对应的缓解措施。

恶意参与者对智能合约基础设施发起恶意攻击

对于 Maker 协议来说，最大的风险之一就是恶意参与者。例如，有程序员发现已经部署的智能合约中存在漏洞，然后利用这个漏洞来攻击协议，或是窃取系统中的资产。

在最糟糕的情况下，在协议中充当担保物的所有去中心化数字资产都会被盗，而且无法恢复。

缓解措施：Maker 基金会的第一要务是[维护 Maker 协议的安全性](#)，而 Maker 协议最坚固的防线是形式化验证（Formal Verification）。Dai 代码库是第一个[经过形式验证的去中心化应用代码库](#)。

除了形式系统验证之外，与区块链行业中最顶尖的安全组织签订安全审计合约、组织第三方（独立）审计和 Bug 赏金计划都是 Maker [基金会的安全路线图](#)。可以访问 Maker 的[多担保 Dai 安全性报告 Github 库](#)，查看形式化验证报告和 Maker 协议的审计报告。

这些安全措施形成了一个强大的防御系统；然而，这个系统绝非天衣无缝。即使经过了形式化验证，对预期行为的数学建模也有可能存在问题，或者对预期行为的假设本身也有可能是错误的

黑天鹅事件

黑天鹅事件指的是系统所遭受的罕见而严重的突然袭击。Maker 协议可能会遭受下列黑天鹅事件：

- 用来生成 Dai 的担保物遭到攻击
- 一种或多种担保物的价格出现意外暴跌
- 高度串谋的喂价机攻击
- 恶意的 Maker 治理提议

注，上述“黑天鹅事件”并不详尽，其排列也不反映可能性程度。

缓解措施：虽然没有一个解决方案是万全的，但是谨慎设计的 Maker 协议（清算率、债务上限、治理安全模块、预言机安全模块、紧急关停等）搭配良好的治理（例如，对危机的迅速应对、周全的风险参数等）有助于防止及缓解攻击所产生的严重影响。

无法预见的定价错误和市场的非理性

信息输入机制的喂价问题和非理性的市场动态会导致 Dai 的价格在较长一段时间内发生波动。如果用户对系统失去信心，即使利率调整和 MKR 增发达到极端的水平，也无法为市场带来足够的流动性和稳定性。

缓解措施：Maker 治理聚集了足够大的资金池来激励看护者，以此实现理性和市场效率的最大化，让 Dai 的供应量在不受市场冲击的情况下稳定增加。紧急关停是最后一道防线。一旦紧急关停被激活，Dai 持有者可以用目标价格赎回担保物。

用户转向了更简单的方案

Maker 协议是一个复杂的去中心化系统。由于 Maker 系统较为复杂，毫无经验的密码学货币用户可能会放弃该系统，转向更容易使用和理解的系统。

缓解措施：虽然对于大多数加密货币爱好者和用于保证金交易的看护者来说，Dai 是很容易生成和使用的，但是新用户可能会觉得 Maker 协议难以理解和使用。虽然从设计层面上来说，用户不需要理解 Maker 协议的底层机制就可以通过 Dai 来获利，Maker 社区和 Maker 基金会一直在提供尽可能简单的文档和[各种资源](#)来引导新用户。

Maker 基金会解散

Maker 基金会当前的目标是，与独立的参与者一起维护 Maker 协议并在全球范围内推广其应用，同时促进治理流程。但是，根据 Maker 基金会的计划，一旦 MakerDAO 可以完全实现自我治理，Maker 基金会就会解散。如果 MakerDAO 在 Maker 基金会的解散之后无法独挑大梁，Maker 协议未来的健康发展将遭受威胁。

缓解措施：在 Maker 项目实现“渐进式去中心化”之后，基金会的解散并不会影响 MKR 持有者的利益。此外，对 Maker 系统的成功管理将带来充足的治理资金，用以持续维护并改善 Maker 协议。

实验性技术的一般问题

Maker 协议的用户（包括但不限于 Dai 和 MKR 持有者）了解并接受 Maker 协议所采用的软件、技术乃至理论都是未经证明的，也无法保证该技术不会中断或出错。一个固有风险是，技术上的弱点、缺陷或漏洞会导致 Maker 协议和/或其构成部分完全崩溃。

缓解措施：参见上文“不良参与者对智能合约基础设施发起恶意攻击”一节。缓解措施的部分解释了技术审计是如何确保 Maker 协议如预期般运行的。

价格稳定性机制

Dai 的目标价格

Dai 的目标价格被用来确定 Dai 持有者在紧急关停情况下收到的担保物的价值。Dai 是 1:1 软锚定美元的，因此其目标价格是 1 美元。

紧急关停

紧急关停（也可简称为关停）主要有两个目的。首先，它是发生紧急情况时的最后一道防线，用来保护 Maker 协议免受基础设施的攻击并直接执行 Dai 的目标价格。紧急情况包括恶意治理行为、非法入侵、安全漏洞和长期市场非理性。其次，关停被用来促进 Maker 协议系统的升级。关停流程只能由 Maker 治理控制。

MKR 投票者也可以通过在紧急关停模块（Emergency Shutdown Module, ESM）中存入 MKR 来立即触发紧急关停，只要有足够多投票者认为有必要即可。这可以防止（激活状态下的）治理安全性模块推迟关停提议的执行。在紧急关停模块中，只要达到一定的票数，关停就会立即生效。

紧急关停的三个阶段：

1. Maker 协议关闭；金库所有者取回资产

一旦关停启动，用户就无法再创建新的金库或操控已创建的金库，喂价机制也会冻结。冻结喂价机制可以确保所有用户都能取回其应得的资产净值。Maker 金库的所有者可以立即取回金库中超过为债务担保所需的担保物。

2. 紧急关停后的拍卖流程

关停被触发之后，担保物拍卖开始，且必须在特定时间段内完成。这个时间段是由 Maker 治理决定的，比最长的担保物拍卖期限略长一些。这可以保证，在拍卖流程结束之时，所有拍卖都能完成。

3. Dai 持有者赎回剩余的担保物

在拍卖流程结束之后，Dai 持有者直接按照固定的汇率用 Dai 赎回担保物，即，基于 Dai 的目标价格来赎回担保物。例如，假设 ETH/USD 汇率是 200 : 1。紧急关停启动之时，某个用户持有 1000 Dai，按照 1 美元的目标价格来计算，该用户在拍卖流程结束之后可赎回 5 ETH。赎回是有限期的。Dai 持有者将以一定比例赎回担保物组合中的每种担保物。要注意的是，Dai 持有者可能会蒙受损失，无法以 1 美元的目标价格全部兑付他们持有的 Dai。一方面是因为担保物贬值带来的风险，另一方面是因为金库持有者有权在 Dai 持有者赎回剩余担保物之前有权取回多余的担保物。关于紧急关停的详细信息，包括优先赎回权，参见[已发布的社区文档](#)。

Maker 协议的未来：大规模采用并实现完全去中心化

潜在市场

对于很多去中心化应用来说，价格稳定的加密货币是一种重要的交换媒介。Dai 的潜在市场绝不亚于整个去中心化区块链行业。但是，Dai 的目标远不止于此，还要扩展到其他行业。

以下列出了当前稳定币 Dai 市场的一部分：

- **周转资金、对冲和杠杆交易。** Maker 金库允许用户进行免许可型交易，用户可以通过 金库担保生成 Dai 来作为周转资金。迄今为止，有数以万计的金库所有者将 ETH 作为担保物生成了 Dai，再用 Dai 来购买 ETH，从而实现了全额担保型杠杆交易。
- **商业收据、跨境交易和汇款。** Dai 可以降低外汇的波动性并免去对中介的需求，这意味着跨国交易的成本会大幅降低。
- **慈善机构和非政府组织。** 它们可以使用透明的分布式账本技术。
- **游戏业。** 对于区块链游戏开发者来说，Dai 是一种理想的货币之选。整合了 Dai 之后，游戏开发者得到的不仅是一种货币，还有一个经济系统。有了 Dai 的可组合性，游戏开发者可以基于去中心化金融构建新的玩家行为机制。
- **预测市场。** 在做出不相关的预测时，使用波动性较强的密码学货币会增加下注的风险。下注者必须考虑到这类资产未来价格波动的风险，因此不可能去参与较为远期的事件预测。稳定币 Dai 是预测市场的天然之选。

资产扩张

MKR 持有者也许愿意将新的资产纳入担保物类别，这些资产也将受到 Dai 的风险要求、参数和安全措施（例如，清算率、稳定费、存款利率和债务上限等）的约束。

发展信息输入机制

MakerDAO 是以太坊区块链上首个运行可靠的信息输入机制项目。因此，许多去中心化应用都使用 MakerDAO 喂价机制来确保系统的安全性，并持续提供最新的价格数据。有了 MakerDAO 和 Maker 协议提供的保障，Maker 治理可以拓宽核心的信息输入机制基础设施，从而更好地适应去中心化应用的需求。

总结

Maker 协议允许用户生成 Dai，即，一种完全存在于区块链上的、价格稳定的价值贮藏物。Dai 是一种去中心化稳定币，不由任何中心化的参与者或存在信任风险的中介方和对手方发行或管理。它是一视同仁的，不受国界的限制——可由世界各地的任何人获得。

所有 Dai 都是通过超额担保生成的，且担保物是被托管到经过审核且公开可见的以太坊智能合约中的。只要有网络连接，任何人随时都能在 daistats.com 上监控系统的健康状况。

MakerDAO 在密码学货币领域拥有数百位合作伙伴，以及最强大的开发者社区之一，已经成为了去中心化金融（DeFi）运动的引擎。Maker 正在释放区块链的力量，来实现当代对经济赋能的期望。

了解更多信息，请访问 [MakerDAO 官网](https://makerdao.com)。

附录

使用 Dai 的优势和示例

Maker 协议对世界各地的所有人开放，不受任何限制或个人信息要求的约束。以下列举了 Dai 在全世界范围内的一些用例。

Dai 给每个人提供财务独立的机会

根据世界银行（World Bank）发布的《2017 全球普惠金融指数报告》（Global Findex Database 2017），全球大约有 17 亿人口没有银行账户⁵。根据联邦存款保险公司（FDIC）在 2017 年进行的一项调查，仅在美国就有大约 3200 万家庭无法享受银行服务或没有充分享受银行服务⁶，即，他们完全没有银行账户，或通常使用其他方式来代替传统的银行业（例如，发薪日贷款和典当贷款）来管理他们的财务。Dai 可以为这类人群赋能；他们只需要联上互联网即可。

作为全球首个中立的稳定币，Dai 给任何人提供财务独立的机会，不受他们所处的地理位置和环境的影响。例如，在拉丁美洲地区，Dai 可以帮助个人和家庭对冲阿根廷比索⁷和委内瑞拉玻利瓦尔的贬值。在南太平洋的瓦努阿图岛，那里的居民需要支付很高的转账费。位于英国的非营利组织国际乐施会（Oxfam International）、澳大利亚的创业公司 Sempo、以太坊创业公司 ConsenSys 在埃法特岛上成功试行了一项现金援助计划，向岛上的 200 位居民每人发了 50 Dai，在当地供应商网络中充当一种支付媒介⁸。

自我主权货币的生成

用户可以通过 Oasis Borrow 来访问 Maker 协议，并在 Maker 金库中锁定担保物来生成 Dai。用户不需要访问任何第三方中介来生成 Dai。金库让个人和企业有机会以简单快捷的方式和较低的成本来担保资产并生成流动性。

自动获得存款收益

世界各地的 Dai 持有者都可以利用 Dai 存款利率来更好地接入金融系统。正如上文所述，Dai 存款利率建立在 Dai 的价值之上，允许用户利用自己所持有的 Dai 来赚钱，保护自己的存款不受通货膨胀的影响。

例如，假设 Bob 在 DSR 合约中锁定了 10 万个 Dai，Maker 治理将 DSR 的年利率设定在 6%，则 Bob 一年可赚取 6000 Dai 的存款收益。此外，由于交易所和区块链项目可以将 DSR 整合进自己的平台，这给加密货币交易者、企业家和知名企业带来了新的机会，可以增加他们持有的 Dai 存款和营运资本。由于这种有吸引力的机制，Market Maker（做市商）可能会选择长期持有 Dai，并将其锁入 DSR。

快捷的低成本汇款

无论是购买商品或服务，还是向家庭和朋友转账，跨境汇款都需要支付高昂的服务费和转账费，等待较长的转账时间，克服因通货膨胀而产生的汇率问题。世界各地的人都将稳定币 Dai 作为一种交换媒介，因为他们相信 Dai 的价值和效率。

Dai 可以给汇款用户带来以下好处：

- **低成本的国内和国际转账。** Dai 可以立即节省成本，用较低的以太坊网络矿工费代替较高的银行转账费。较低的成本还有助于提高交易频率。
- **全天候服务。** Dai 的运营时间与银行不同。Maker 协议是全天候开放的。
- **便捷的出/入口。** 用户可以利用许多法币出口/入口来实现法币和 Dai 之间的交易。这些选择可以帮助用户在法币和密码学货币之间搭建桥梁，轻而易举地将他们持有的 Dai 兑换成当地的货币。
- **更强的安全性和信心。** 区块链提供了更高的安全性，可以加深消费者的信任。

高波动市场中的稳定性

正如上文所指出的那样，Dai 既是一种很容易获得的价值贮藏物，也是一种强大的交换媒介。它可以保护交易者免受波动性的影响。例如，它可以让交易者简单流畅地控制仓位，在市场中保持活跃，无需通过法币出/入口反复进行法币交易。

Dai 推动了生态系统的发展并建立去中心化金融

随着越来越多的用户意识到稳定币 Dai 的价值，更多开发者正在将 Dai 整合进他们构建在以太坊区块链上的 dApp。Dai 有助于构建一个更加强大的生态系统。简而言之，dApp 开发者可以将 Dai 作为一种稳定的交换媒介提供给他们用户，代替那些投机性资产来买卖商品和服务。

此外，由于 Dai 可以在以太坊生态系统中被用来支付以太坊网络矿工费，开发者可通过创建接受 Dai 而非 ETH 的 DeFi dApp 来为用户提供更加流畅的引导体验和更好的综合体验。

术语

- [MakerDAO 术语表](#)
- [Maker 协议术语表](#) (术语、变量、功能等)

系统和社区资源

- [MakerDAO on GitHub](#)
- [MakerDAO Documentation](#)
- [MakerDAO.com](#)
- [The MakerDAO Blog](#)
- [The MakerDAO Forum](#)
- [The MakerDAO Chat](#)
- [MakerDAO on Reddit](#)
- [MakerDAO on Twitter](#)
- [MakerDAO on Weibo](#)

脚注

1. 在以太坊社区中，去中心化自治组织（DAO）指的是围绕某个特定的目标和项目而创建的社会和科技社区，并不一定以传统公司的形式存在。↵

2. <https://ethereum.org/> ↵

3. <https://www.jpmorgan.com/global/news/digital-coin-payments> ↵

4. https://libra.org/en-US/wp-content/uploads/sites/23/2019/06/LibraWhitePaper_en_US.pdf ↵

5. <https://globalindex.worldbank.org/> ↵

6. <https://www.fdic.gov/householdsurvey/> ↵

7. <https://slideslive.com/38920018/living-on-defi-how-i-survive-argentinas-50-inflation> ↵

8. <https://www.coindesk.com/oxfam-trials-delivery-of-disaster-relief-using-ethereum-stablecoin-dai> ↵

(完)